PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 6 : H04L 9/32

A1

(11) Numéro de publication internationale: WO 97/13342

(43) Date de publication internationale: 10 avril 1997 (10.04.97)

(21) Numéro de la demande internationale: PCT/FR96/01546

(22) Date de dépôt international: 3 octobre 1996 (03.10.96)

(30) Données relatives à la priorité:
95/11622 3 octobre 1995 (03.10.95) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: GEMPLUS S.C.A. [FR/FR]; Avenue du Pic-de-Bretagne, Parc d'activités de Gémenos, Boîte postale 100, F-13881 Gémenos Cédex (FR).

(72) Inventeurs; et
(75) Inventeurs/Déposants *(US seulement)*: M'RAIHI, David [FR/FR]; 30, rue Basfroi, F-75011 Paris (FR). NACCACHE, David [FR/FR]; 7, rue Chaptal, F-75009 Paris (FR). STERN, Jacques [FR/FR]; 16, rue Vandrezanne, F-75013 Paris (FR). VAUDENAY, Serge [FR/FR]; 9, rue Grillon, F-75004 Paris (FR).

(74) Mandataire: NONNENMACHER, Bernard; Gemplus S.C.A., Z.I. Athelia III, Voie Antiope, F-13705 La Ciotat (FR).

(81) Etats désignés: JP, US, brevet européen (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Publiée
Avec rapport de recherche internationale.
Avant l'expiration du délai prévu pour la modification des revendications, sera republiée si de telles modifications sont reçues.

(54) Title: PUBLIC KEY CRYPTOGRAPHY PROCESS BASED ON THE DISCRETE LOGARITHM

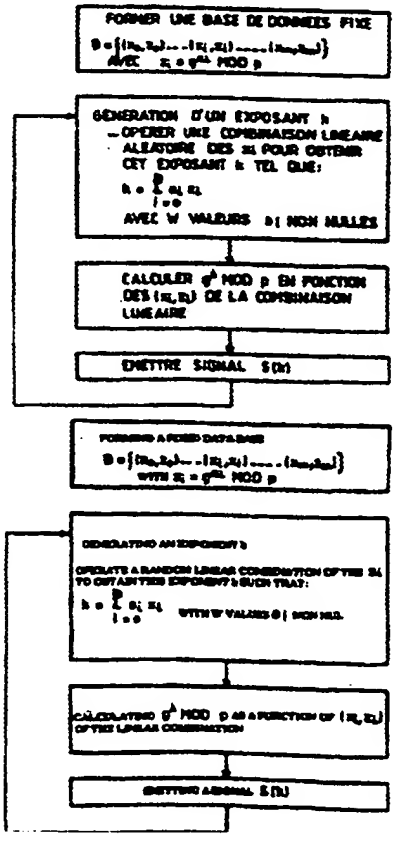
(54) Titre: PROCEDE DE CRYPTOGRAPHIE A CLE PUBLIQUE BASE SUR LE LOGARITHME DISCRET

(57) Abstract

The invention relates to a cryptography process with public key, based on the discrete logarithm and implying the calculation of the magnitude $r = g^k \bmod p$, wherein p is an integer called modulus, and k is a random number. According to the invention, a data base comprising the couples (x_i, $g^{x_i} \bmod p$) is formed, the x_i being pseudo-random values and said values are used in a linear combination in order to obtain an exponent k, the calculation of the magnitude $g^k \bmod p$ being done by using the g^{x_i} entering in the combination. Application to the digital signature or to the authentication.

(57) Abrégé

L'invention a pour objet un procédé de cryptographie à clé publique basé sur le logarithme discret faisant intervenir le calcul de la grandeur $r = g^k \bmod p$ où p est un nombre premier appelé module, k un nombre aléatoire. Selon l'invention on forme une base de données comprenant des couples (x_i, $g^{x_i} \bmod p$), les x_i étant des valeurs pseudo-aléatoires et on utilise ces valeurs dans une combinaison linéaire pour obtenir un exposant k, le calcul de la grandeur $g^k \bmod p$ se faisant en utilisant les g^{x_i} entrant dans la combinaison. Application à la signature numérique ou à l'authentification.



UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AT	Arménie	GB	Royaume-Uni	MW	Malawi
AT	Autriche	GE	Géorgie	MX	Mexique
AU	Australie	GN	Guinée	NE	Niger
BB	Barbade	GR	Grèce	NL	Pays-Bas
BE	Belgique	HU	Hongrie	NO	Norvège
BF	Burkina Faso	IE	Irlande	NZ	Nouvelle-Zélande
BG	Bulgarie	IT	Italie	PL	Pologne
BJ	Bénin	JP	Japon	PT	Portugal
BR	Brésil	KE	Kenya	RO	Roumanie
BY	Bélarus	KG	Kirghizistan	RU	Fédération de Russie
CA	Canada	KP	République populaire démocratique de Corée	SD	Soudan
CF	République centrafricaine	KR	République de Corée	SE	Suède
CG	Congo	KZ	Kazakhstan	SG	Singapour
CH	Suisse	LI	Liechtenstein	SI	Slovénie
CI	Côte d'Ivoire	LK	Sri Lanka	SK	Slovaquie
CM	Cameroun	LR	Libéria	SN	Sénégal
CN	Chine	LT	Lituanie	SZ	Swaziland
CS	Tchécoslovaquie	LU	Luxembourg	TD	Tchad
CZ	République tchèque	LV	Lettonie	TG	Togo
DE	Allemagne	MC	Monaco	TJ	Tadjikistan
DK	Danemark	MD	République de Moldova	TT	Trinité-et-Tobago
EE	Estonie	MG	Madagascar	UA	Ukraine
ES	Espagne	ML	Mali	UG	Ouganda
FI	Finlande	MN	Mongolie	US	Etats-Unis d'Amérique
FR	France	MR	Mauritanie	UZ	Ouzbékistan
GA	Gabon			VN	Viet Nam

PROCÉDÉ DE CRYPTOGRAPHIE A CLÉ PUBLIQUE BASÉ SUR LE LOGARITHME DISCRET

La présente invention a pour objet un procédé de cryptographie dite à clé publique basé sur le logarithme discret faisant intervenir le calcul d'une grandeur modulo p.

Elle trouve une application dans la génération de signatures numériques de messages, ou dans une cession d'authentification entre deux entités .

Dans de telles procédures, la sécurité est fondée sur l'extrême difficulté qu'il y a à inverser certaines fonctions et plus particulièrement le logarithme discret.

Ce problème consiste, étant donné la relation mathématique $y = g^x$ modulo p que l'on notera par la suite $y = g^x \bmod p$ (qui signifie y est le reste de la division de g^x par p), à retrouver x lorsque l'on connaît p, g et y. Ce problème est impossible à résoudre, en l'état actuel des connaissances, dès que la taille p atteint ou dépasse 512 bits et que celle de x atteint ou dépasse 128 bits.

Dans de tels systèmes, il existe en général une autorité qui fournit le nombre p de grande taille, constituant le module. L'autorité choisit également un entier g, appelé base tel que l'ensemble engendré par g c'est-à-dire l'ensemble formé des nombres $g^x \bmod p$, pour x appartenant à l'intervalle [0, p-1] soit un sous-ensemble de taille maximale, au moins 2^{128}.

Les paramètres p et g sont dits "publics" c'est-à-dire qu'ils sont fournis par l'autorité à tous les utilisateurs rattachés à cette autorité.

Selon certaines variantes, ces paramètres sont choisis individuellement par chaque utilisateur et

font, dans ce cas, partie intégrante de sa clé publique.

Un inconvénient majeur à la mise en oeuvre de systèmes cryptographiques réside dans la nécessité d'avoir des moyens de calcul et de mémorisation relativement importants du fait des calculs complexes qui sont réalisés.

En effet, le calcul de la grandeur $g^k \text{mod} p$ consiste à réaliser des multiplications modulaires et cela est coûteux en temps de calcul et en place mémoire. Dans des dispositifs électroniques simples n'utilisant que des microprocesseurs standards, ce type d'opération n'est guère réalisable.

Pour des dispositifs électroniques possédant un processeur spécialisé pour ce type de calcul, il est malgré tout souhaitable de limiter, le temps de calcul et la place mémoire nécessaire pour les résultats intermédiaires.

En effet, le calcul de la grandeur $g^k \text{mod} p$ est en général relativement coûteux par la méthode classique du "carré-multiplié" connue sous l'abréviation anglo-saxonne SQM (Square-Multiply) puisqu'il équivaut en moyenne à $3/2\ \text{Log}_2(p)$ multiplications.

Selon cette méthode on calcule toutes les puissances de g c'est à dire, lorsque k est de longueur n bits, tous les carrés :

$$g^{2^0},\ g^{2^1},\ \ldots\ g^{2^n},$$

Selon la méthode du "carré multiplié" simple g^k requiert n/2 multiplications et n carrés.

Une méthode proposée par E. BRICKELL et al. dénommée par l'abréviation BGCW permet de réduire le nombre de multiplications dans le cas de la méthode du

carré-multiplié mais introduit un besoin de stockage de nombreuses constantes précalculées et donc la nécessité de disposer d'une quantité de mémoires de stockage très pénalisante.

La présente invention a pour objet de remédier à tous ces inconvénients. Elle permet d'apporter une solution souple et peu onéreuse en temps de calcul et en place mémoire à la mise en oeuvre d'algorithmes cryptographiques pour tous systèmes de cryptographie et en particulier par des appareils portables du type carte à puce à microprocesseur.

Selon l'invention deux solutions sont proposées. Les deux solutions sont basées sur un principe commun consistant à constituer une base de données de valeurs aléatoires et à combiner ces valeurs pour déterminer des exposants k servant aux échanges entre deux entités.

Avec les deux solutions proposées, le calcul d'un exposant k requiert moins de 30 multiplications modulaires pour un espace mémoire tout à fait acceptable pour des supports tels que les cartes à puce.

L'invention a plus particulièrement pour objet un procédé de cryptographie à clé publique basé sur le logarithme discret faisant intervenir le calcul de la grandeur $r = g^k \bmod p$ ou p est un nombre premier appelé module, l'exposant k un nombre aléatoire habituellement de longueur N bits et g un entier appelé base, dans lequel une entité E réalise des opérations d'authentification et/ou de signature, comprenant des échanges de signaux avec une autre entité dans lesquels

intervient cette grandeur, caractérisé en ce qu'il comporte les étapes suivantes pour une entité donnée :

- former une base de données contenant un nombre fixe d'exposants et les puissances correspondantes,

puis pour chaque échange de signaux:

- générer un exposant en opérant une combinaison linéaire aléatoire des valeurs d'exposant de la base,
- et calculer la puissance de g à partir des puissances de la base entrant dans la combinaison.

Selon un premier mode de réalisation, les étapes consistent à:

- former une base de données fixe contenant m valeurs x_i aléatoires et les grandeurs correspondantes z_i telles que $z_i = g^{xi} \bmod p$,
- générer un exposant k nécessaire à chaque signature en opérant une combinaison linéaire aléatoire des valeurs x_i de la base,
- calculer la grandeur $g^k \bmod p$ à partir des grandeurs z_i relatives aux valeurs x_i intervenant dans la combinaison,
- utiliser cette grandeur dans les échanges de signaux avec une autre entité.

Selon un deuxième mode de réalisation, les étapes consiste à :

- former une base de données évolutive contenant n valeurs aléatoires d'exposants et leur puissance (k_i, $g^{k_i} \bmod p$)
- générer un nouvel exposant k_{i+1} nécessaire à une signature en opérant une combinaison linéaire aléatoire des n valeurs k_i ,

- calculer la grandeur g^{k}_{i+1} modp en réalisant le produit des puissances de g^{k} de la combinaison linéaire,

- mettre à jour la base des exposants et des puissances,

- utiliser cette grandeur dans les échanges de signaux avec une autre entité.

D'autres particularités et avantages de l'invention apparaîtront à la lecture de la description qui est faite et qui est donnée à titre d'exemple illustratif et non limitatif en regard des dessins qui représentent :

- la figure 1, un schéma de principe d'un système apte à mettre en oeuvre l'invention,

- la figure 2, un schéma fonctionnel représentant les étapes essentielles du procédé selon l'invention,

- la figure 3, le schéma fonctionnel selon un premier mode de réalisation,

- la figure 4, le schéma fonctionnel selon un deuxième mode de réalisation.

On a représenté sur la figure 1, un schéma de principe d'un système de mise en oeuvre du procédé de cryptographie objet de l'invention.

Ce système est formé d'une entité E1 désirant effectuer des échanges de signaux électroniques avec au moins une autre entité E2. les deux entités sont munies respectivement d'une unité de traitement (CPU) 11, 30, d'une interface de communication, d'une mémoire vive (RAM) 13, 32 et/ou d'une mémoire non inscriptible (ROM) 14, 34 et/ou d'une mémoire non volatile inscriptible ou réinscriptible (EPROM ou EEPROM) 15, 33 et un bus d'adresses, de données, de contrôle 16, 35.

L'unité de commande de traitement et/ou la ROM contiennent des programmes ou des ressources de calcul correspondant à l'exécution des étapes de calcul intervenant dans le procédé objet de l'invention, c'est-à-dire lors d'une session d'authentification ou lors de la génération d'une signature électronique ou au cours desquelles les deux entités s'échangent des signaux électroniques.

L'unité de traitement ou la ROM possèdent les ressources nécessaires à des multiplications, additions et réductions modulaires.

De même que l'unité de traitement et/ou la ROM comportent les fonctions de cryptographie utilisées propres à chaque algorithme de cryptographie et les paramètres g et p, nécessaires au calcul et fixés un fois pour toute pour la suite. Les exposants x_i selon le premier mode ou k_i selon le deuxième mode pourront être chargés au préalable dans une mémoire réinscriptible, par l'autorité ou, générés à partir d'un générateur aléatoire et d'une valeur aléatoire source x_0 (ou k_0) secrète. Chaque entité E1, E2 possède en outre une clé secrète x et la clé publique y.

L'invention s'applique tout particulièrement aux systèmes à cryptographie mis en place dans le domaine bancaire où une grande sécurité est requise lors de transactions opérées sur les comptes.

C'est aussi le cas où l'on désire authentifier l'envoi de messages transmis sous forme de signaux électroniques envoyés par une autre entité.

C'est aussi le cas où l'on a besoin de signer des messages lors d'échanges de signaux avec une autre entité.

En pratique, l'entité désireuse de réaliser une transaction pourra être, par exemple, une carte à

circuit intégré telle qu'une carte à puce et l'entité destinataire sera alors un terminal bancaire.

La suite de la description va être faite dans le cadre de l'application du procédé à la signature de messages numériques, étant bien entendu que l'invention s'applique à tout système de cryptographie basé sur le logarithme discret.

La figure 1, illustre les étapes essentielles du procédé. Selon l'invention on forme une une base de données contenant un nombre fixe d'exposants et les puissances correspondantes,

puis pour chaque échange de signaux:

- on génère un exposant en opérant une combinaison linéaire aléatoire des valeurs d'exposant de la base,
- et on calcule la puissance de g à partir des puissances de la base entrant dans la combinaison.

Le procédé selon l'invention propose deux solutions reposant toutes deux sur la formation (ou constitution) de cette base de données.

Selon le premier mode de réalisation, la base est fixe et est formée d'un ensemble de m couples (x_i, z_i). Les données x_i sont des nombres aléatoires obtenus comme dit précédemment par un générateur de nombres aléatoires ou pseudo-aléatoires. La longueur de ces nombres est celle d'un exposant k et est la même pour tous (soit N bits). Les grandeurs z_i sont le résultat d'un calcul préalable tel que :

$$z_i = g^{x_i} \bmod p.$$

La longueur des grandeurs z_i est celle du modulo p.

Lorsque l'entité E1 possède cette base de données $B = [(x_0, z_0), \ldots (x_{m-1}, -z_{m-1})]$, elle peut échanger des signaux avec une autre entité en faisant intervenir par exemple une signature DSA (r, s) telle que $r = g^k \bmod p$ dans laquelle k a été généré à partir des données de la base B.

Ainsi selon l'invention, l'entité génère un exposant k lorsque cela est nécessaire et elle le fait en réalisant une combinaison linéaire aléatoire des valeurs x_i de la base. L'entité calcule ensuite la grandeur $g^k \bmod p$ correspondante.

Pour la génération de l'exposant k, l'entité procède de la manière suivante :

- l'entité génère une séquence de valeurs a_i: $(a_0, \ldots, a_{m-1})$ qui sont des nombres entiers aléatoires tels que $0 \leq a_i \leq h$ et parmi lesquels w valeurs seulement sont non nulles.
- l'entité génère k de sorte que :

$$k = \sum_{i=0}^{m-1} a_i \, x_i$$

- l'entité calcule ensuite la grandeur $g^k \bmod p$ en opérant les multiplications des puissances de g données par les valeurs z_i relatives aux x_i qui entrent dans la combinaison linéaire. En pratique les x_i entrant dans la combinaison linéaire sont ceux pour lesquels le coefficient a_i est non nul.

On utilise l'algorithme de BRICKELL et al. pour réaliser ce calcul, mais le nombre de multiplications est désormais $(h/h+1)\ w + h-2$ au lieu de $(h/h+1)\ m + h-2$.

Le nombre w est fixé par rapport à la sécurité requise et conduit aux résultats suivants pour des valeurs de m et h :

m=32, w=24 et h=8

m=64, w=20 et h=6

Ces valeurs sont données à titre d'exemple et on peut envisager diverses combinaisons dès lors que l'on respecte les contraintes de sécurité.

Dans le cas où m=64 et w=20, le nombre de multiplications nécessaires selon l'invention est de 34 alors qu'avec une méthode telle que BRICKELL on aurait 60 multiplications à réaliser.

Pour m=32, on stocke par conséquent 32 nombres de taille du module p soit 512 à 1024 bits suivant le cas et 32 nombres de 160 bits (N=160).

Les m couples (x_i, z_i) seront stockés en mémoire EEPROM dans le cas où l'entité est une carte et cela de façon protégé par les méthodes habituelles de blindage et analogue.

La deuxième solution proposée selon l'invention consiste à former une base de données évolutive à partir de n valeurs aléatoires d'exposants k_i, i=1 à n et de leur puissance g^{ki} modp.

Une première nouvelle valeur d'exposant k_{i+1} est ensuite obtenue par combinaison linéaire aléatoire des exposants de la base. Le calcul de la grandeur $g^{k_{i+1}}$ correspondant à ce nouvel exposant est effectué. Ce nouveau couple est introduit dans la base de données en remplacement du premier.

Un exposant k nécessaire à une signature est obtenu par combinaison linéaire de tous les autres exposants

de la base et le contenu de la base est modifié à chaque nouvelle génération d'un exposant.

En effet, on remet à jour la base en remplaçant le premier couple par le dernier obtenu.

Ainsi à l'instant t, la base est de la forme:

((k_o, g^{k_o} modp), (k_1, g^{k_1} modp),....

...., (k_t, g^{k_t} modp))

on calcule alors k_{t+1} et on met à jour la base qui devient:

((k_1, g^{k_1} modp), (k_2, g^{k_2} modp),....

...., (k_t, g^{k_t} modp), (k_{t+1}, $g^{k_{t+1}}$ modp))

le processus se répète à chaque calcul d'un nouveau k dans la séquence pseudo aléatoire.

Chaque exposant de la base est une combinaison linéaire exprimé pour la relation suivante :

$$k_t = \sum_{i=0}^{h-1} a_i \, k_{t+i-(h-1)};$$

avec h-1 = n

dans laquelle les coefficients a_i sont des nombres entiers positifs, aléatoires.

Les nombres aléatoires sont obtenus à partir d'une séquence fixe a_0, ..., a_{h-1} sur laquelle on effectue une permutation aléatoire.

Ainsi, la génération d'un exposant k_{t+1} peut s'exprimer par la relation suivante :

$$k_{t+1} = l_t[k_{(t+i-(h-1)}, \ldots, k_t]$$

l_t étant une fonctionnelle linéaire (linear functional) à coefficients entiers, choisie au hasard parmi L fonctionnelles .

Les coefficients a_i sont des petites puissances de 2. On choisit des valeurs prises entre 1 et 2^f avec f ayant une taille qui permet une implémentation

efficace. On choisira par exemple f=7 afin de rester cohérent avec les valeurs proposées par l'algorithme de Schnorr. On prendra donc la suite 0, ..., a_{h-1} comme une permutation aléatoire de la séquence $(1, 2, \ldots, 2^7)$.

Les coefficients des combinaisons linéaires doivent être inférieurs à une valeur seuil b pour éviter des attaques et conserver les k_t uniformément distribués et (h-1)-indépendant.

En considérant h et $L=b^h$, on suggère les valeurs h=8 et b=4 et on fixe $L=\{1, \ldots, b\}^h$.

La taille des nombres k est généralement de 160 bits. Dans ce cas le nombre de multiplications modulaires intervenant selon le procédé de l'invention est nettement inférieur au nombre de multiplications généralement constaté dans l'état de l'art actuel. En effet il est pour les valeurs retenues, inférieur à 30.

REVENDICATIONS

1. Procédé de cryptographie à clé publique basé sur le logarithme discret faisant intervenir le calcul de la grandeur $r = g^K$ modp ou p est un nombre premier appelé module, k un nombre aléatoire habituellement de longueur N bits et g un entier appelé base, dans lequel une entité E réalise des opérations d'authentification et/ou de signature, comprenant des échanges de signaux avec une autre entité dans lesquels intervient cette grandeur, procédé comportant les étapes suivantes pour une entité donnée :
- former une base de données contenant un nombre fixe d'exposants et les puissances correspondantes, puis pour chaque échange de signaux :
- générer un exposant en opérant une combinaison linéaire aléatoire des valeurs d'exposant de la base,
- et calculer la puissance de g à partir des puissances de la base entrant dans la combinaison,
les dites étapes consistant à :
- former une base de données fixe contenant m valeurs x_i aléatoires et les grandeurs correspondantes z_i telles que $z_i = g^{xi}$ modp,
- générer un exposant k nécessaire à chaque signature en opérant une combinaison linéaire aléatoire des valeurs x_i de la base,
- calculer la grandeur g^K modp à partir des grandeurs z_i relatives aux valeurs x_i intervenant dans la combinaison,
- utiliser cette grandeur dans les échanges de signaux avec une autre entité,

ledit procédé étant caractérisé en ce que la génération des grandeurs k comporte les autres étapes suivantes :
- générer un exposant k tel que $k = \Sigma a_i x_i$ et tel que l'on ait w des m valeurs a_i non nulles, le choix des a_i non nuls étant obtenu de façon aléatoire,
- calculer la grandeur g^Kmodp en utilisant les valeurs z_i correspondant aux valeurs x_i qui entrent dans la combinaison linéaire de k.

2. Procédé de cryptographie selon la revendication 1, caractérisé en ce que pour former la base de données dans une entité, on effectue les étapes suivantes :
- générer m valeurs aléatoires x_i de N bits à partir d'un générateur pseudo-aléatoire, et d'une valeur initiale secrète x_0,

- calculer la grandeur $z_i = g^{xi}$ modp en réalisant le produit des puissances de g modulo p entrant dans la combinaison linéaire selon laquelle peut être décomposée une valeur x_i,
- stocker en mémoire non volatile de l'entité les m couples (x_i, z_i).

3. Procédé de cryptographie à clé publique selon la revendication 1, caractérisé en ce que les étapes consistent à :
- former une base de données évolutive contenant n valeurs aléatoires d'exposants et de leur puissance $(k_i, g^{Ki}$ modp)
- générer un nouvel exposant k_{i+1} nécessaire à une signature en opérant une combinaison linéaire aléatoire des n valeurs k_i de la base,
- calculer la grandeur $g^{K\,i+1}$ modp en réalisant le produit des puissances de g entrant dans la combinaison linéaire,
- mettre à jour la base en remplaçant un couple par ce nouveau couple,
- utiliser cette grandeur dans les échanges de signaux avec une autre entité.

4. Procédé de cryptographie selon la revendication 3, caractérisé en ce que pour un exposant k_t de la base, cet exposant est une combinaison linéaire de la forme :

$$k_t = \sum_{i=0}^{h-1} a_i\, k_{t+i-(h-1)};$$

avec $h - 1 = n$

et dans laquelle les coefficients a_i sont des nombres entiers positifs aléatoires.

5. Procédé de cryptographie selon la revendication 3, caractérisée en ce que les coefficients a_i, $i = 0$ à $h - 1$ sont obtenus par une permutation aléatoire d'une séquence fixe.

6. Procédé de cryptographie selon la revendication 5, caractérisé en ce qu'un nouvel exposant k_{t+1} est une combinaison linéaire des autres exposants s'exprimant par la relation :

$$k_{t+1} = l_t (k_{t+i-(h-1)}, \ldots, k_t) ,$$

et l_t une fonctionnelle linéaire.

7. Procédé de cryptographie selon l'une quelconque des revendications précédentes caractérisé en ce qu'il peut être mis en oeuvre pour des cartes à microprocesseur.

FIG_1

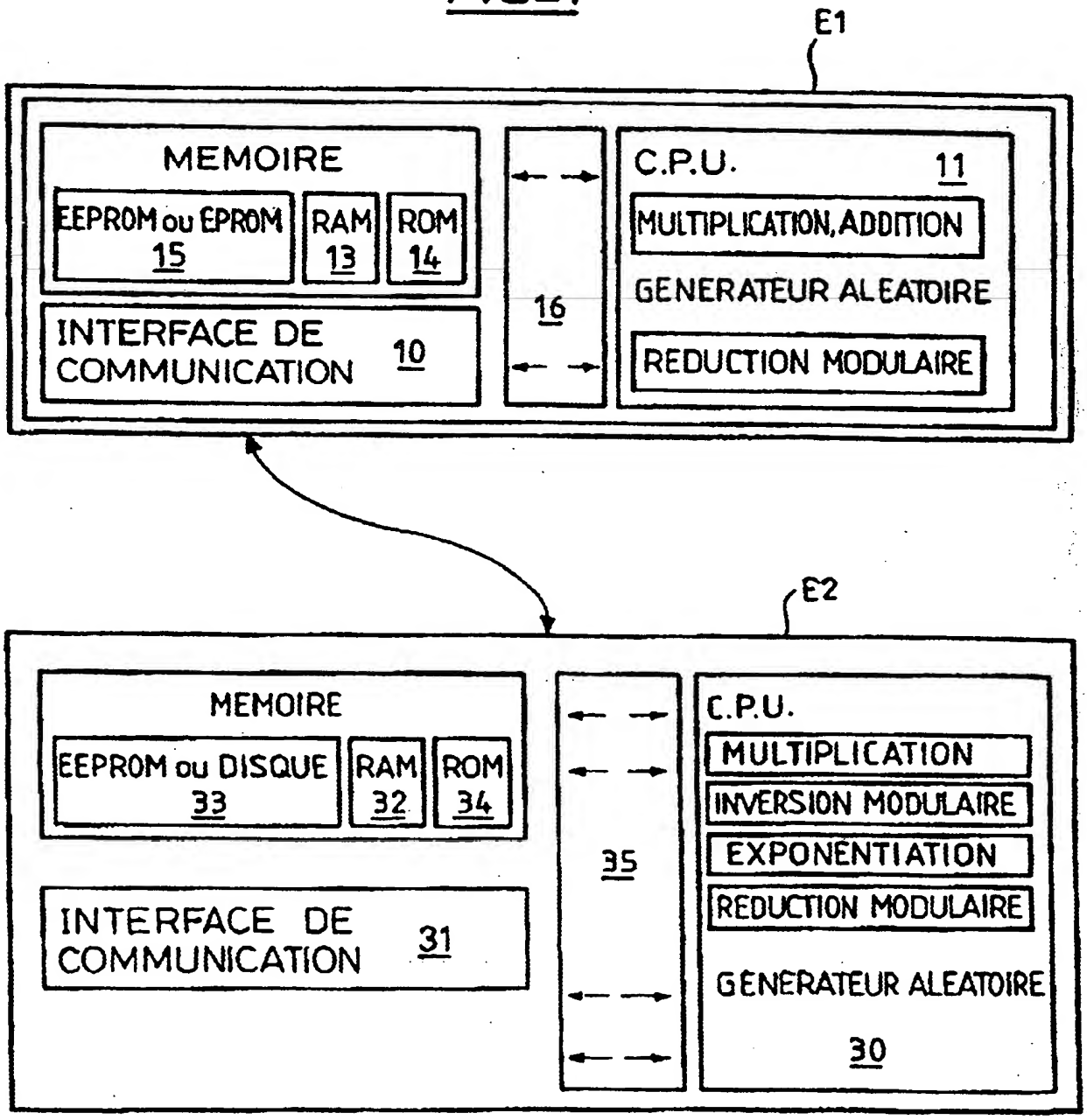

E1
MEMOIRE
EEPROM ou EPROM 15
RAM 13
ROM 14
INTERFACE DE COMMUNICATION 10
16
C.P.U. 11
MULTIPLICATION, ADDITION
GENERATEUR ALEATOIRE
REDUCTION MODULAIRE
E2
MEMOIRE
EEPROM ou DISQUE 33
RAM 32
ROM 34
INTERFACE DE COMMUNICATION 31
35
C.P.U.
MULTIPLICATION
INVERSION MODULAIRE
EXPONENTIATION
REDUCTION MODULAIRE
GENERATEUR ALEATOIRE 30

FIG_2

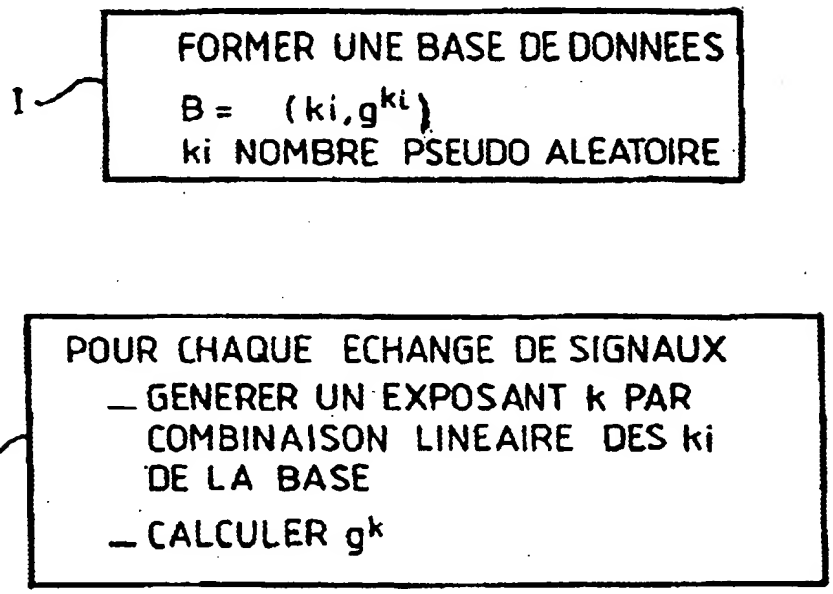

I
FORMER UNE BASE DE DONNEES
B = (ki, g^ki)
ki NOMBRE PSEUDO ALEATOIRE
II
POUR CHAQUE ECHANGE DE SIGNAUX
_ GENERER UN EXPOSANT k PAR COMBINAISON LINEAIRE DES ki DE LA BASE
_ CALCULER g^k

FIG_3

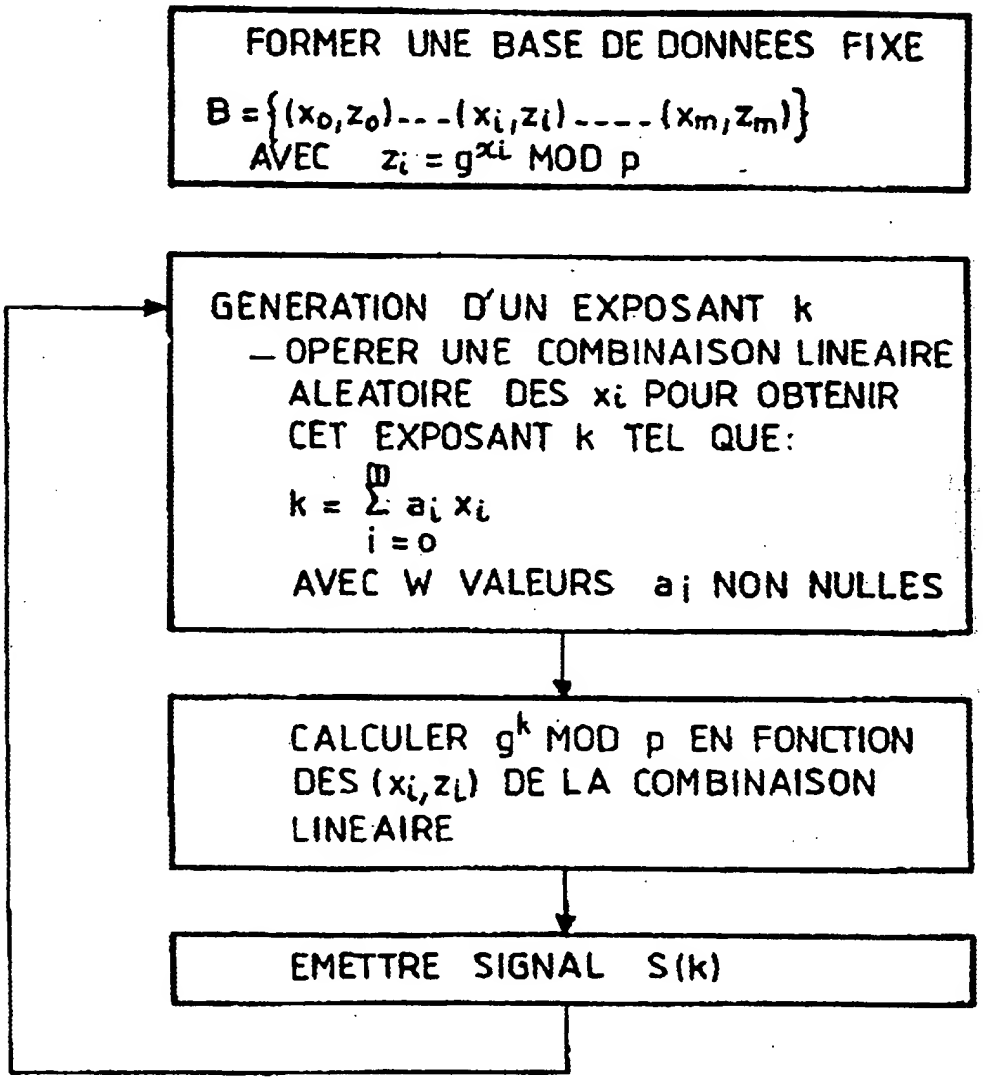
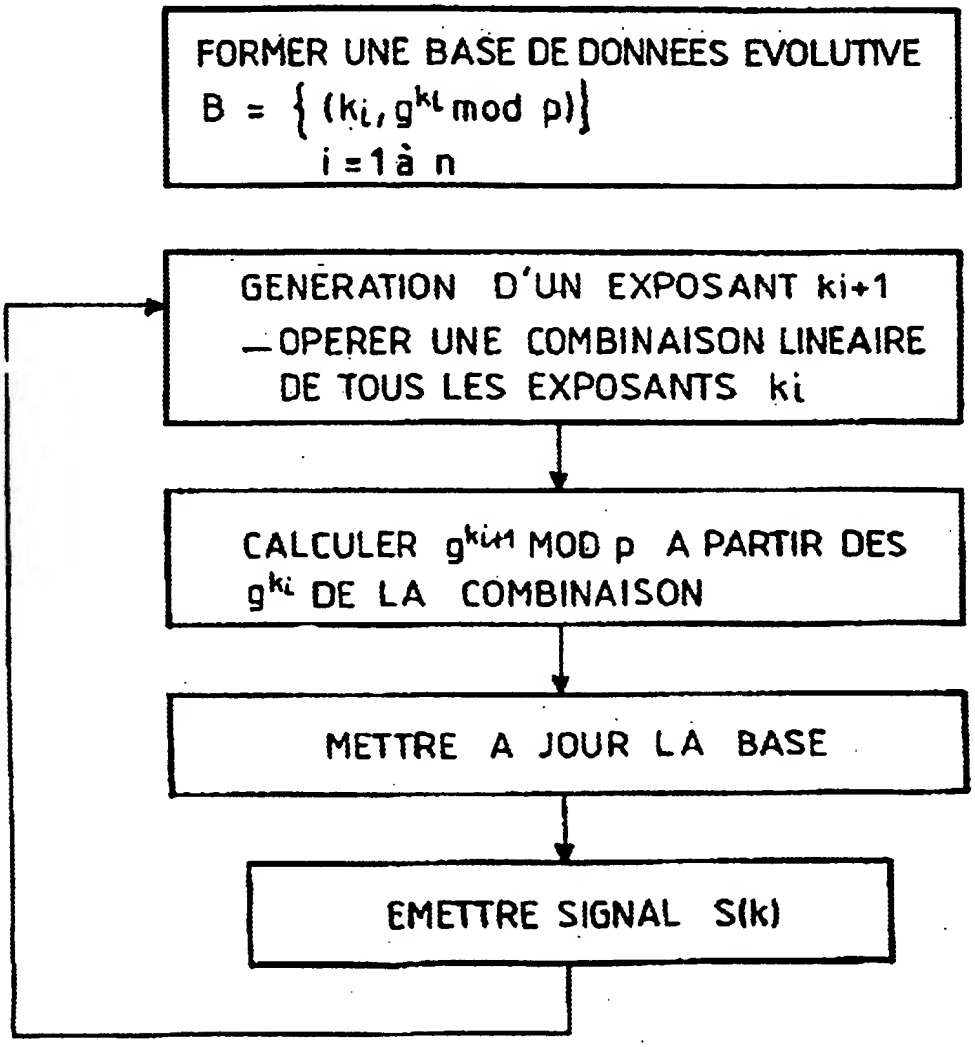

FORMER UNE BASE DE DONNEES FIXE
$B = \{(x_0, z_0) \ldots (x_i, z_i) \ldots (x_m, z_m)\}$
AVEC $z_i = g^{x_i} \text{ MOD } p$
GENERATION D'UN EXPOSANT k
– OPERER UNE COMBINAISON LINEAIRE ALEATOIRE DES x_i POUR OBTENIR CET EXPOSANT k TEL QUE:
$k = \sum_{i=0}^{m} a_i x_i$
AVEC W VALEURS a_i NON NULLES
CALCULER g^k MOD p EN FONCTION DES (x_i, z_i) DE LA COMBINAISON LINEAIRE
EMETTRE SIGNAL S(k)

FIG_4


FORMER UNE BASE DE DONNEES EVOLUTIVE
B = { (ki, g^ki mod p) }
i = 1 à n
GENERATION D'UN EXPOSANT ki+1
— OPERER UNE COMBINAISON LINEAIRE DE TOUS LES EXPOSANTS ki
CALCULER g^ki+1 MOD p A PARTIR DES g^ki DE LA COMBINAISON
METTRE A JOUR LA BASE
EMETTRE SIGNAL S(k)

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/FR 96/01546

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	ADVANCES IN CRYPTOLOGY - EUROCRYPT '92. WORKSHOP ON THE THEORY AND APPLICATIONS OF CRYPTOGRAPHIC TECHNIQUES. PROCEEDINGS, BALATONFURED, HUNGARY, 24-28 MAY 1992, ISBN 3-540-56413-6, 1993, BERLIN, GERMANY, SPRINGER-VERLAG, GERMANY, pages 200-207, XP000577415 BRICKELL E F ET AL: "Fast exponentiation with precomputation" see page 201, line 27 - page 202, line 6 --- -/--	1

[X] Further documents are listed in the continuation of box C.

[ ] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

2

Date of the actual completion of the international search	Date of mailing of the international search report
9 January 1997	28.01.97

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Holper, G

INTERNATIONAL SEARCH REPORT

Inter mal Application No
PCT/FR 96/01546

C(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	AT&T TECHNICAL JOURNAL, NOV.-DEC. 1991, USA, vol. 70, no. 6, ISSN 8756-2324, pages 73-86, XP000256991 BRICKELL E F ET AL: "Interactive identification and digital signatures" Panel 2. Faster Exponentiation see page 79 ---	1
A	JOURNAL OF CRYPTOLOGY, 1991, USA, vol. 4, no. 3, ISSN 0933-2790, pages 161-174, XP002006211 SCHNORR C P: "Efficient signature generation by smart cards" see page 172, line 6 - last line -----	1-3,7

2

RAPPORT DE RECHERCHE INTERNATIONALE

Den : Internationale No
PCT/FR 96/01546

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 6 H04L9/32

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 6 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	ADVANCES IN CRYPTOLOGY - EUROCRYPT '92. WORKSHOP ON THE THEORY AND APPLICATIONS OF CRYPTOGRAPHIC TECHNIQUES. PROCEEDINGS, BALATONFURED, HUNGARY, 24-28 MAY 1992, ISBN 3-540-56413-6, 1993, BERLIN, GERMANY, SPRINGER-VERLAG, GERMANY, pages 200-207, XP000577415 BRICKELL E F ET AL: "Fast exponentiation with precomputation" voir page 201, ligne 27 - page 202, ligne 6 --- -/--	1

[X] Voir la suite du cadre C pour la fin de la liste des documents

[ ] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
9 Janvier 1997	28.01.97

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl, Fax (+ 31-70) 340-3016	Holper, G

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Dem. Internationale No
PCT/FR 96/01546

C(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	AT&T TECHNICAL JOURNAL, NOV.-DEC. 1991, USA, vol. 70, no. 6, ISSN 8756-2324, pages 73-86, XP000256991 BRICKELL E F ET AL: "Interactive identification and digital signatures" Panel 2. Faster Exponentiation voir page 79 ---	1
A	JOURNAL OF CRYPTOLOGY, 1991, USA, vol. 4, no. 3, ISSN 0933-2790, pages 161-174, XP002006211 SCHNORR C P: "Efficient signature generation by smart cards" voir page 172, ligne 6 - dernière ligne -----	1-3,7

2